Published on *GamblingCompliance* (https://gamblingcompliance.com)

Cryptos Still Pose Huge AML Risk, Warn Experts

17TH AUG 2020 | WRITTEN BY: HARRISON SAYERS

Cryptocurrencies could yet bolster the fight against money laundering, but with online gambling sites caught up in a massive crypto scam just weeks ago, unregulated digital currency exchanges and tech-savvy scammers still pose a great risk.

“There is no better way to launder money than through crypto,” said Felix Shipkevich, a lawyer and Hofstra University special professor.

The risks that cryptocurrencies present to anti-money laundering (AML) were keenly demonstrated as recently as last month, when more than 100 high-profile Twitter accounts were compromised as part of a Bitcoin scam, with some of the stolen funds routed through gambling sites in an attempt to obscure their origin.

The risks surrounding crypto largely stem from its “early regulatory framework, especially when compared to other currency exchanges such as FOREX”, which Shipkevich says is decades ahead.

“There is still a lot of global ambiguity regarding its regulation,” he said.

For instance, anyone can create a cryptocurrency “relatively easily” and they are used regularly on the dark web, he said.

Shipkevich told VIXIO that he believes the best way to tackle these problems is to regulate cryptocurrencies globally.

Regulation of the sector is stepping up a gear in some jurisdictions. The cryptocurrency industry is currently bracing for a boost to competition, innovation and M&A in light of the Office of the Comptroller of the Currency (OCC) in the United States confirming that national banks and federal savings associations can provide crypto custody services for customers — meaning to keep their digital assets in safekeeping for a fee.

“Providing custody services does not present the same risks as conducting transactions. With that said, banks must meet comprehensive Bank Secrecy Act and anti-money laundering compliance requirements regarding their operations, including those related to providing custody services,” Bryan Hubbard, deputy comptroller for public affairs, told VIXIO.

Regulating cryptos is partly difficult due to its community being “split on the benefits of AML processes and regulations, particularly with regards to the Financial Action Task Force (FATF) travel rules requiring exchanges to keep and hand over client details to regulators”, said Dave Hodgson, chief investment officer at peer-to-peer cryptocurrency and blockchain platform NEM.

The underlying technology of cryptocurrency is “generally censorship-resistant”, but most chains “are not surveillance resistant, particularly when centralised, regulated exchanges are involved”, he added.

When it comes to AML, Hodgson said that cryptos are “clearly significantly stronger” due to blockchain’s ability to audit transactions on-chain compared with the traditional currency, or fiat, system.

However, there have been difficulties identifying tech-savvy individuals who mask their IDs or use unregulated exchanges, with Hodgson pointing out that “many still ask the question: who is Bitcoin’s creator Satoshi Nakamoto?”.

“Crypto idealists dislike the level of surveillance governments seek to place on their citizens, both in crypto and non-crypto domains in the name of security; however, occasionally, they do come in useful for law enforcers. The recent Twitter scamming case is a prime example,” he said.

July’s scam was a serious breach, but showcased law enforcement becoming more adept at using modern tools to investigate crypto-based crimes.

“While investigations into cyber breaches can sometimes take years, our investigators were able to bring these hackers into custody in a matter of weeks,” said John Bennett, the FBI special agent in charge of the investigation.

The perpetrators of the scam were quickly found due in part to tools offered by companies such as Cipher

The perpetrators of the scam were quickly found due in part to tools offered by companies such as Cipher Trace, which can trace crypto transactions.

Authorities were alerted by these tools when the scammers attempted to cash out via regulated crypto exchanges, allowing investigators to subpoena them for know your customer (KYC) data, which included their IDs and addresses.

“Cryptos have been used for a variety of illegal purposes”, but “when combined with known identities, blockchain can facilitate a superior, if not perfect, financial infrastructure”, that is “far more compliant and safer than legacy methods”, according to Jeff Truitt, chief compliance and legal officer at Securrency, developers of blockchain-based financial and regulatory technology.

This is due to fiat money being difficult for authorities to trace back to prior holders, compared with the blockchain ledger recording the entire transaction history of a digital asset, providing information on all of its previous wallet holders, according to Truitt.

“When combined with tools that analyse the proximity of those ancestral digital wallets to wallets previously correlated to a nefarious activity like money laundering, a probabilistic analysis can be made regarding the AML risk of a particular wallet and transaction. This type of nuanced historical analysis is simply not possible with traditional systems,” he said.

TOPICS

Compliance And Risk

Anti-Money Laundering

Payment Methods

Virtual Currencies

GEOGRAPHY

United States

North America

Europe

Asia/Pacific

SECTORS

Online Gambling

CONTENT

Regulatory Insights